REMARKS

The Applicants wish to thank the Examiner for his comments on this case. In response to those comments, the Applicants submit herewith amended claims that are believed to be overcome the objections raised by the Examiner.

It is believed that the basis of the Examiners objections is based upon the interpretation of claim 1 as covering in its scope the computation of a point kP by repeated applications of the Frobenius operator. Such techniques are referenced in the Lercier paper and in the Mullin patent. Claim 1 has been amended to distinguish over such an interpretation by reciting the form of the representation of the scalar k previously recited in claim 4. Such a representation is not taught within the art applied against claim 1 either under 35 USC 102(b) or 35 USC 102(e), both of which reference repeated application of the frobenius operator.

Not only does the method recited in claims 1 and 11 work on a larger class of curves than those methods recited in the prior art but they result in significant increases in efficiency. Simply replacing the Frobenius map in the art with an arbitrary endomorphism does not yield efficient techniques because the resulting expansion may be significantly longer than the binary expansion of k.

Claim 11 has been rewritten as dependent claims corresponding to claims 2 through 9 and therefore overcome the 35 USC 112 objection.

It is believed therefore the present application is now in order for allowance and action to that end is respectfully requested.

Applicant wishes to thank the Examiner for reviewing the present application.

Respectfully Submitted,

John R.S. Orange
Agent for Applicant
Registration No. 29,725